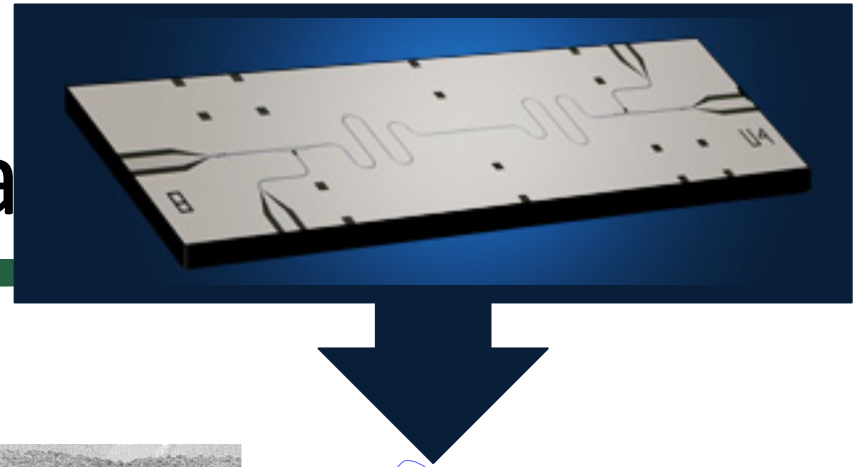
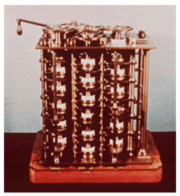
Quantum information as high-dimensional geometry

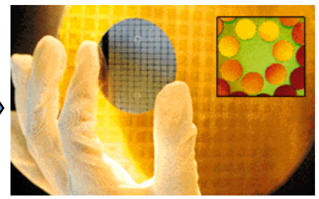
Patrick Hayden
McGill University

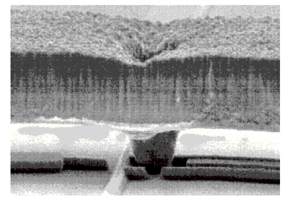
Perspectives in High Dimensions, Cleveland, August 2010

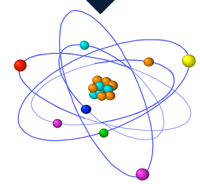
Motiva



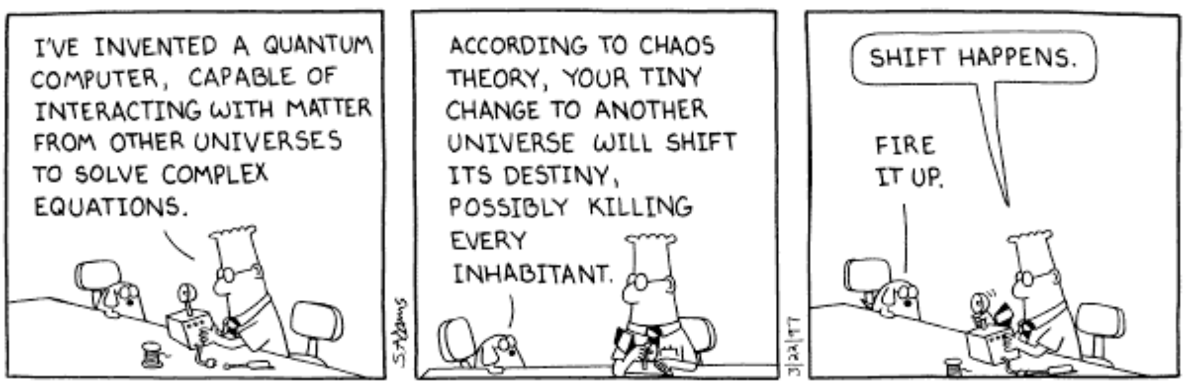








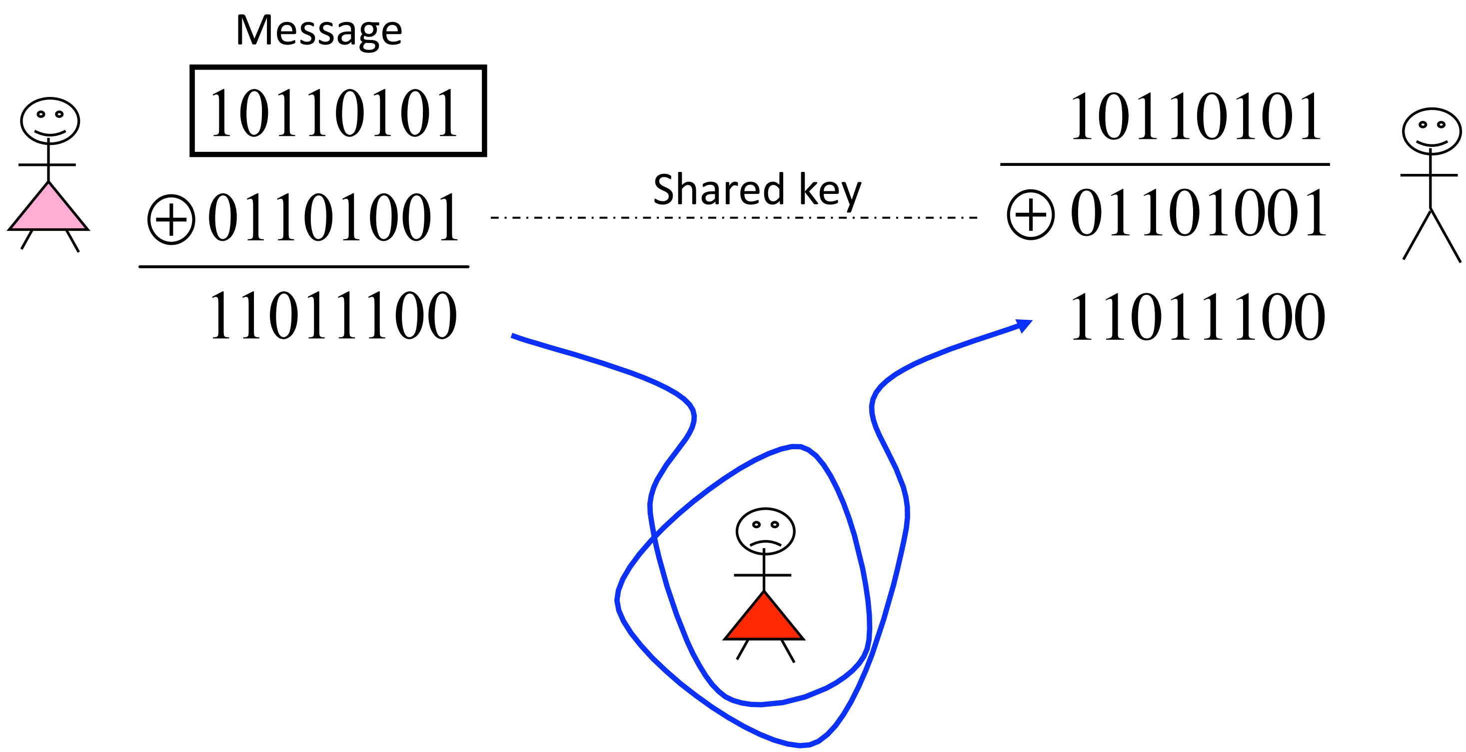
1m .1nm



Outline

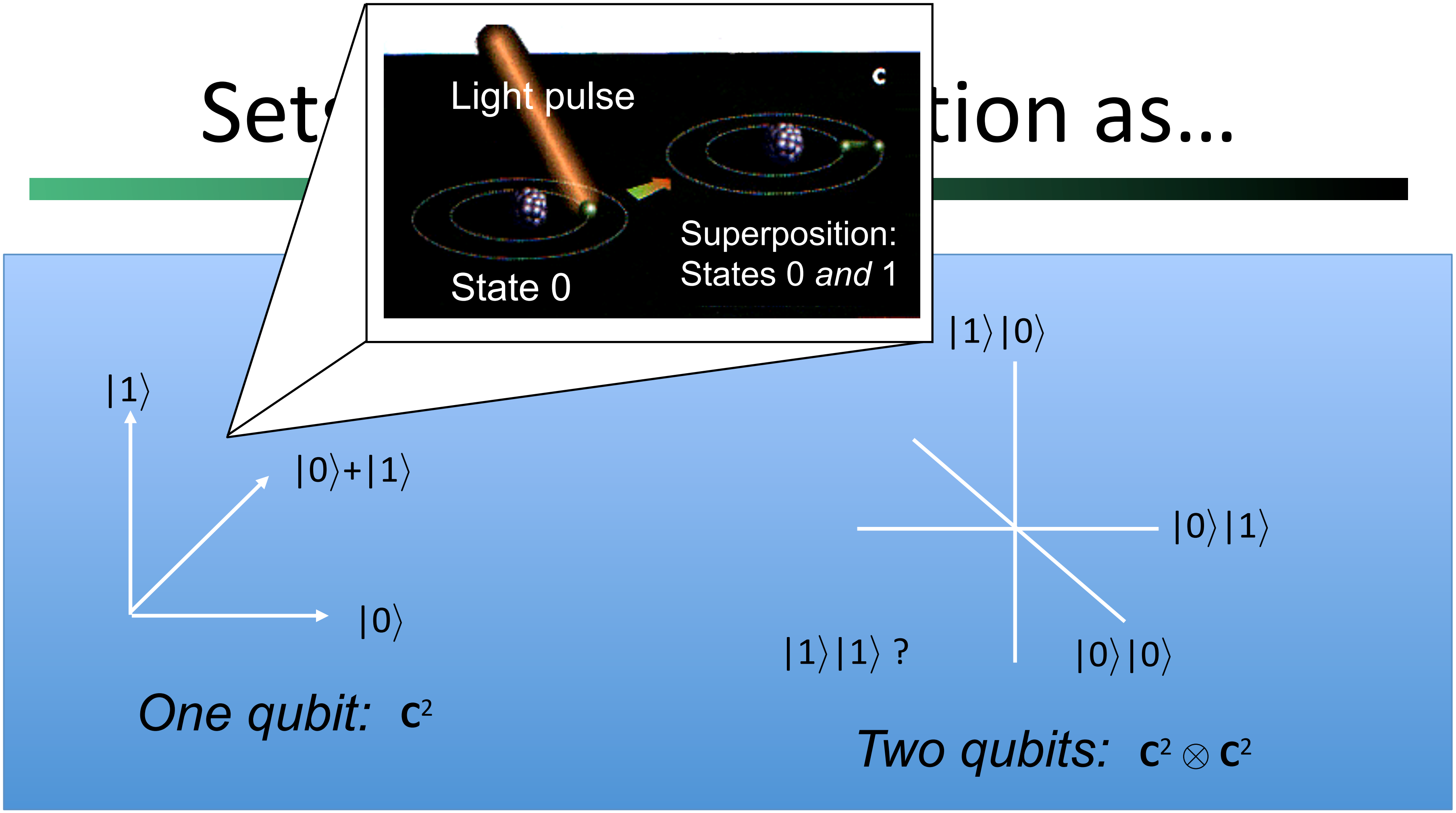
- The one-time pad: classical and quantum
  - Argument from measure concentration
- Superdense coding: from bits to qubits
  - Reduction to Dvoretzky
    - (Almost Euclidean subspaces of Schatten ℓ_p)
- More one-time pad:
  - Exponential (and more) reduction in key size
  - Decomposing $\ell_1(\ell_2)$ into a direct sum of almost Euclidean subspaces

One-time pad



1 bit of key per bit of message necessary and sufficient [Shannon49]

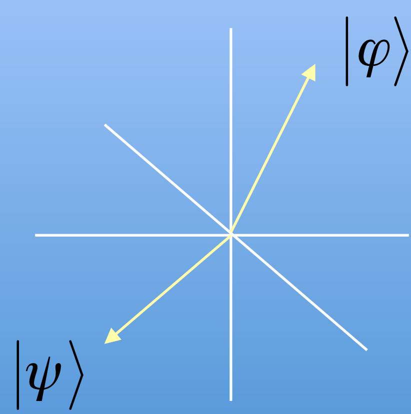
Set tion as...



(Unit) Vectors are to

quantum information.

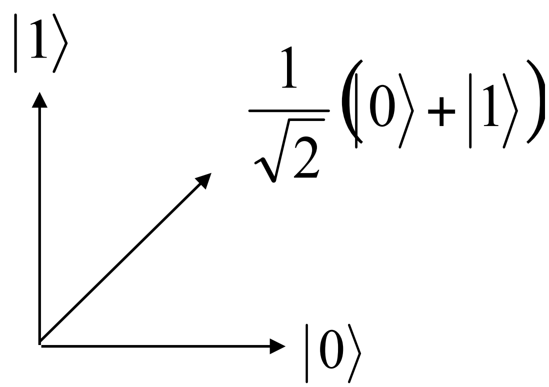
Distinguishability



$\left|\langle\varphi|\psi\rangle\right|$ measures the extent to which

$|\varphi\rangle$ and $|\psi\rangle$ are distinguishable.

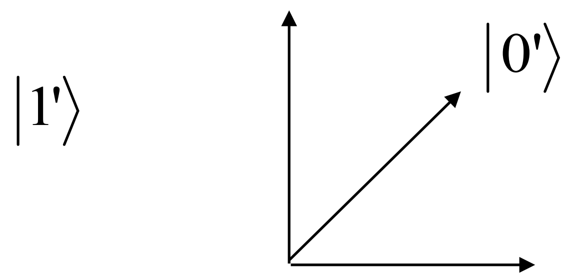
Physical operations…



Are unitary:

They preserve inner products

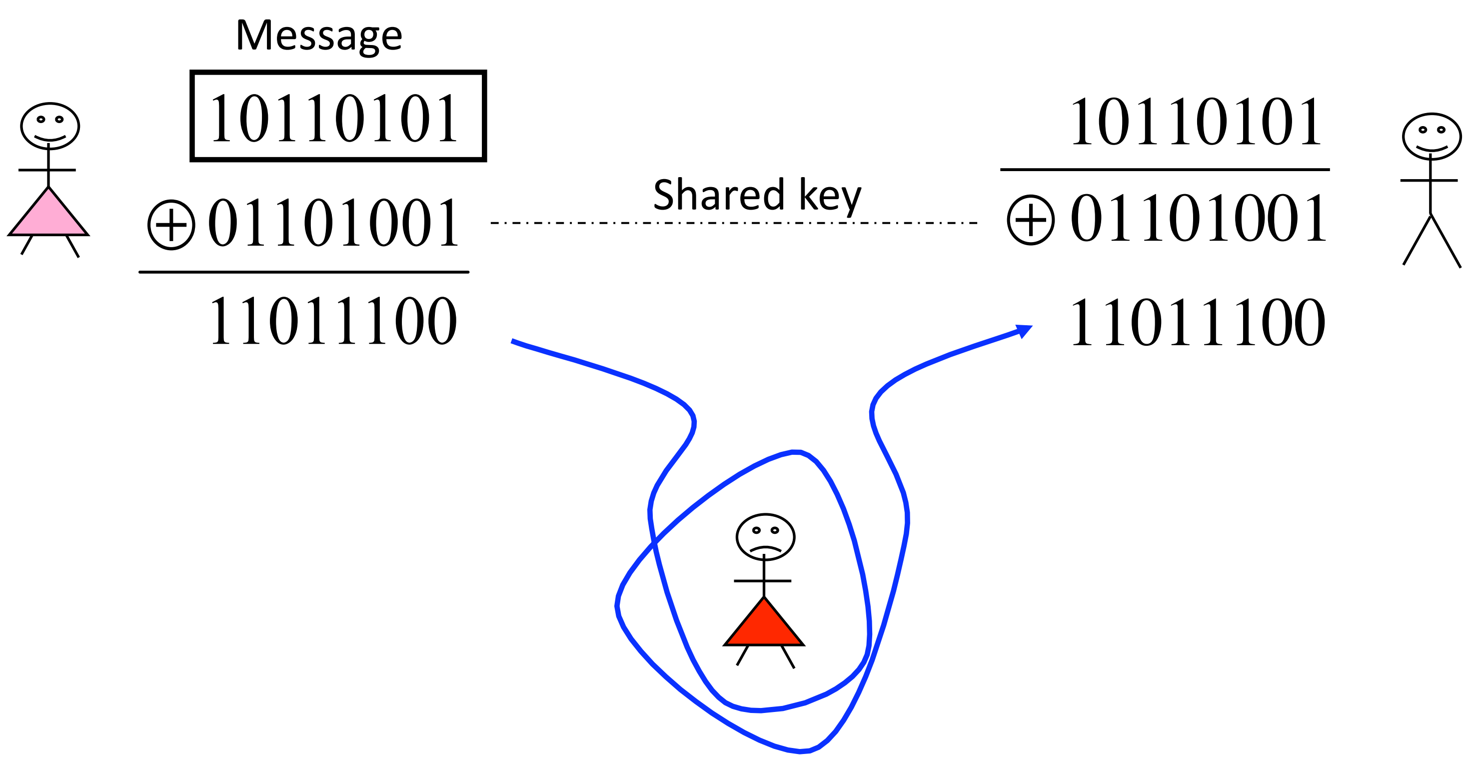
Physical operations…



Are unitary:

They preserve inner products

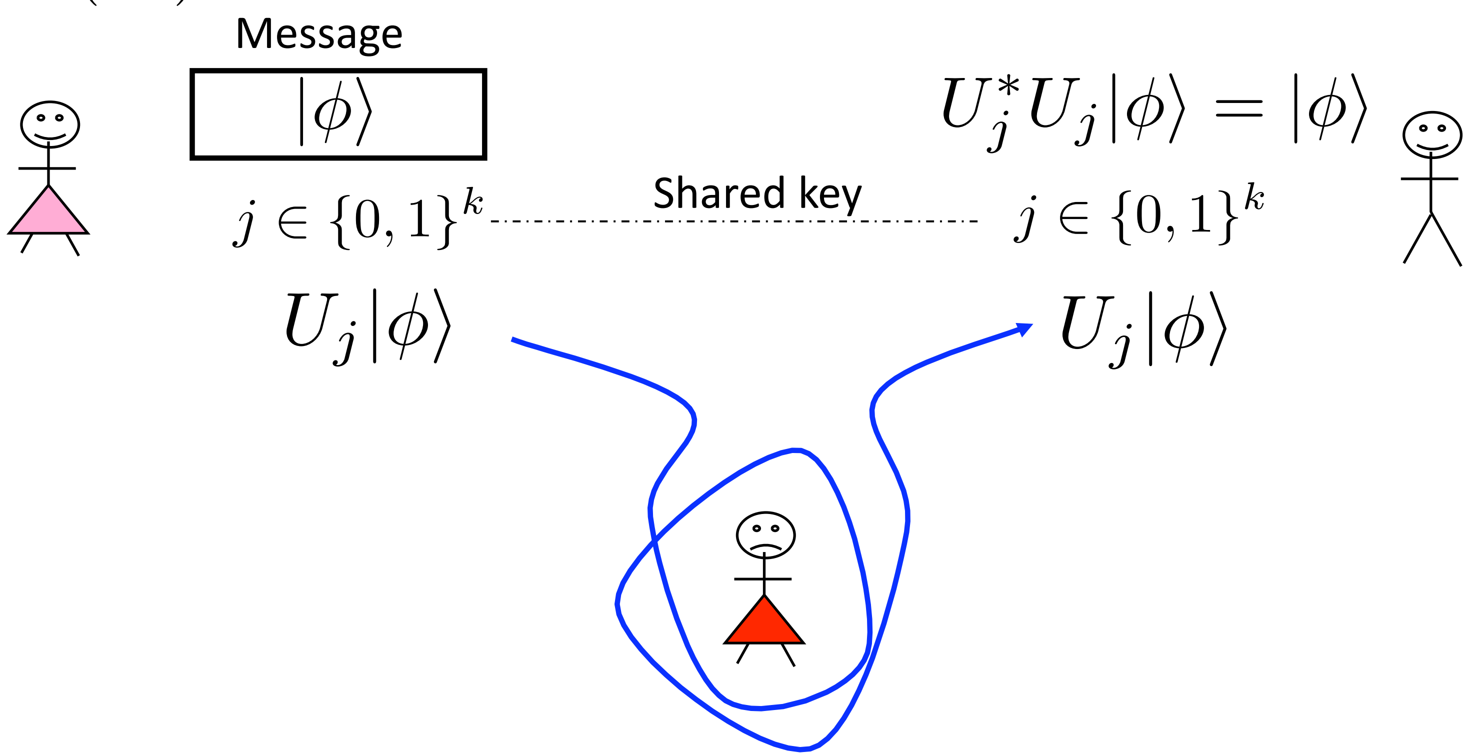
One-time pad



1 bit of key per bit of message necessary and sufficient [Shannon49]

Quantum one-time pad

$\forall |\phi\rangle \in (\mathbb{C}^2)^{\otimes n}$



Security criterion: For all Hermitian X, $\frac{1}{2^k}\sum_j U_j X U_j^* = I \cdot \mathrm{tr}(X)/2^n$

Minimal key length: k = 2n

Approximate quantum one-time pad

Security criterion: For all Hermitian X $\frac{1}{2^k}\sum_j U_j X U_j^* = I \cdot \mathrm{tr}(X)/2^n$

ε-approximate security criterion:

For all Hermitian $X \geq 0, \mathrm{tr}(X) = 1$ $\left\| \frac{1}{2^k}\sum_j U_j X U_j^* - I/2^n \right\|_1 \leq \epsilon$

Schatten norms: if X has singular values $s = (s_i)$, then $\|X\|_p := \|s\|_p$.

- Can achieve using n+log(1/ε^2) bits of key
  - Reduction of factor 2 over exact security
- Proof:
  - Select $\{U_j\}$ i.i.d. according to Haar measure on $U(2^n)$
  - Use net on set of {X}

[H-Leung-Shor-Winter 03]

APPROXIMATE ENCRYPTION: MORE LATER…

Measuring entanglement

Entanglement: nonlocal content of a quantum state (normalized vector)

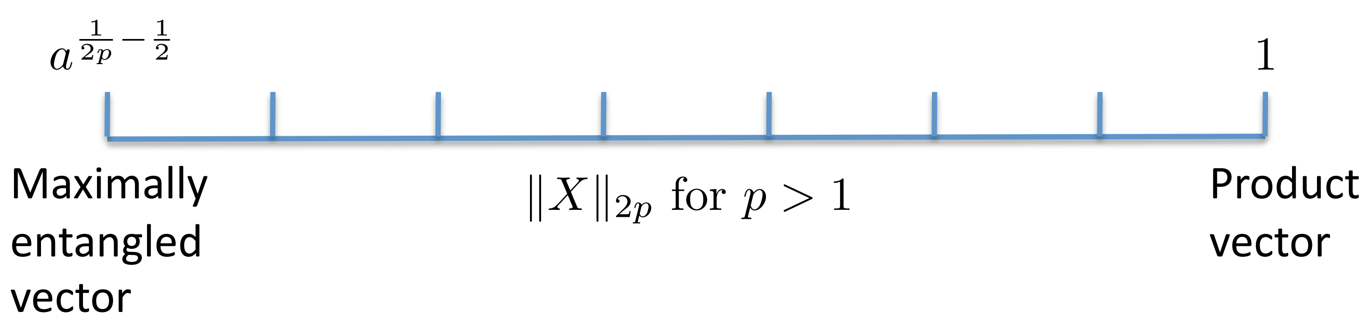
If $x \in \mathbb{C}^a \otimes \mathbb{C}^b$, nonlocal content is orbit of x under $U(\mathbb{C}^a) \times U(\mathbb{C}^b)$.

$$x \mapsto (V \otimes W)x$$

Expand $x = \sum_{i=1}^{a} \sum_{j=1}^{b} x_{ij}\, e_i \otimes f_j$ using orthonormal bases.

If $X = (x_{ij})$, then $X \mapsto VXW^t$ so orbits are labeled by singular values of X.

Schatten norms: if X has singular values $s = (s_i)$, then $\|X\|_p := \|s\|_p$.



Dvoretzky's theorem à la Milman

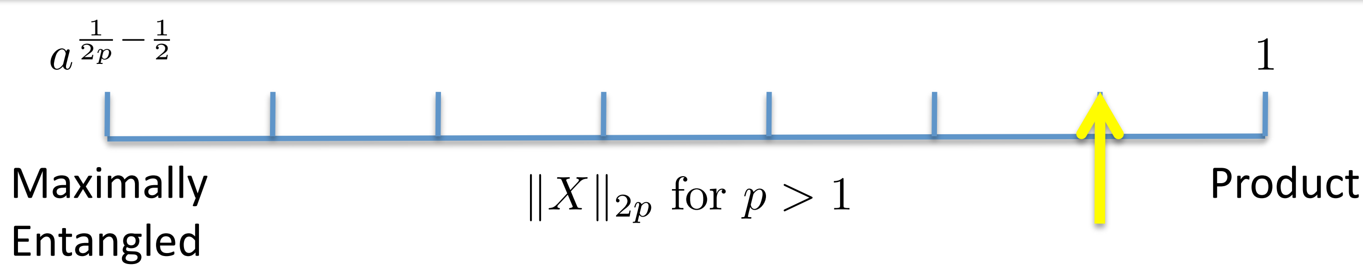
If $a \leq b$, a randomly chosen subspace $S \subset \mathbb{C}^a \otimes \mathbb{C}^b$ of dimension $m \leq c\epsilon^2 a^{1/p} b$ will be such that

$$\|X\|_{2p} \leq (1+\epsilon) a^{\frac{1}{2p}-\frac{1}{2}} (1 + 3\sqrt{a/b}) \|X\|_2$$

for all $X \in S$.

Choose $b = a/\delta$ and restrict to normalized vectors (quantum states).

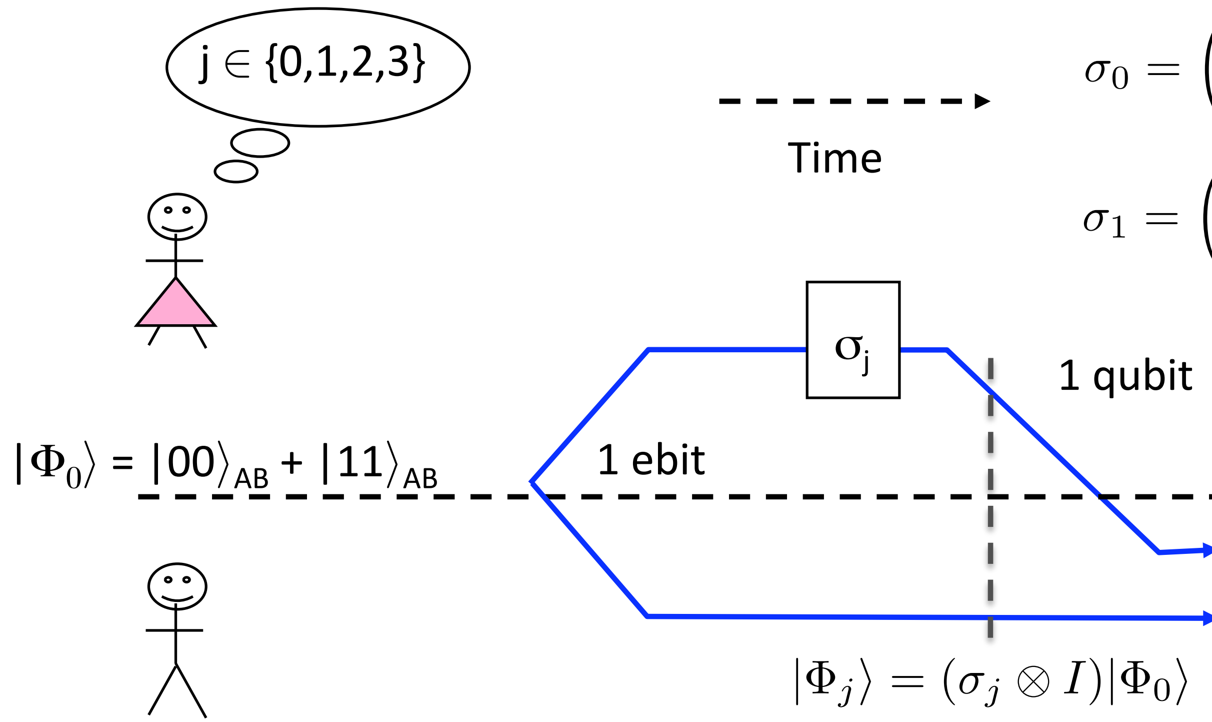
$$\|X\|_{2p} \leq (1+\epsilon) a^{\frac{1}{2p}-\frac{1}{2}} (1 + 3\sqrt{\delta}).$$



For p approaching 1, subspace S is all but constant number of qubits.

[Hayden-Leung-Winter 06, Aubrun-Szarek-Werner 10]

Superdense coding



$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\begin{aligned} |\Phi_0\rangle &= |0\rangle|0\rangle + |1\rangle|1\rangle \\ |\Phi_1\rangle &= |1\rangle|0\rangle + |0\rangle|1\rangle \\ |\Phi_2\rangle &= |1\rangle|0\rangle - |0\rangle|1\rangle \\ |\Phi_3\rangle &= |0\rangle|0\rangle - |1\rangle|1\rangle \end{aligned}$$

Bob receives one of four orthogonal (distinguishable!) states depending on Alice's action

1 ebit + 1 qubit ≥ 2 cbits

[Bennett-Wiesner 92]

Superdense coding of arbitrary quantum states

Suppose that Alice can send Bob an arbitrary 2 qubit state by sharing an ebit and physically transmitting 1 qubit.

1 qubit + 1 ebit ≥ 2 qubits

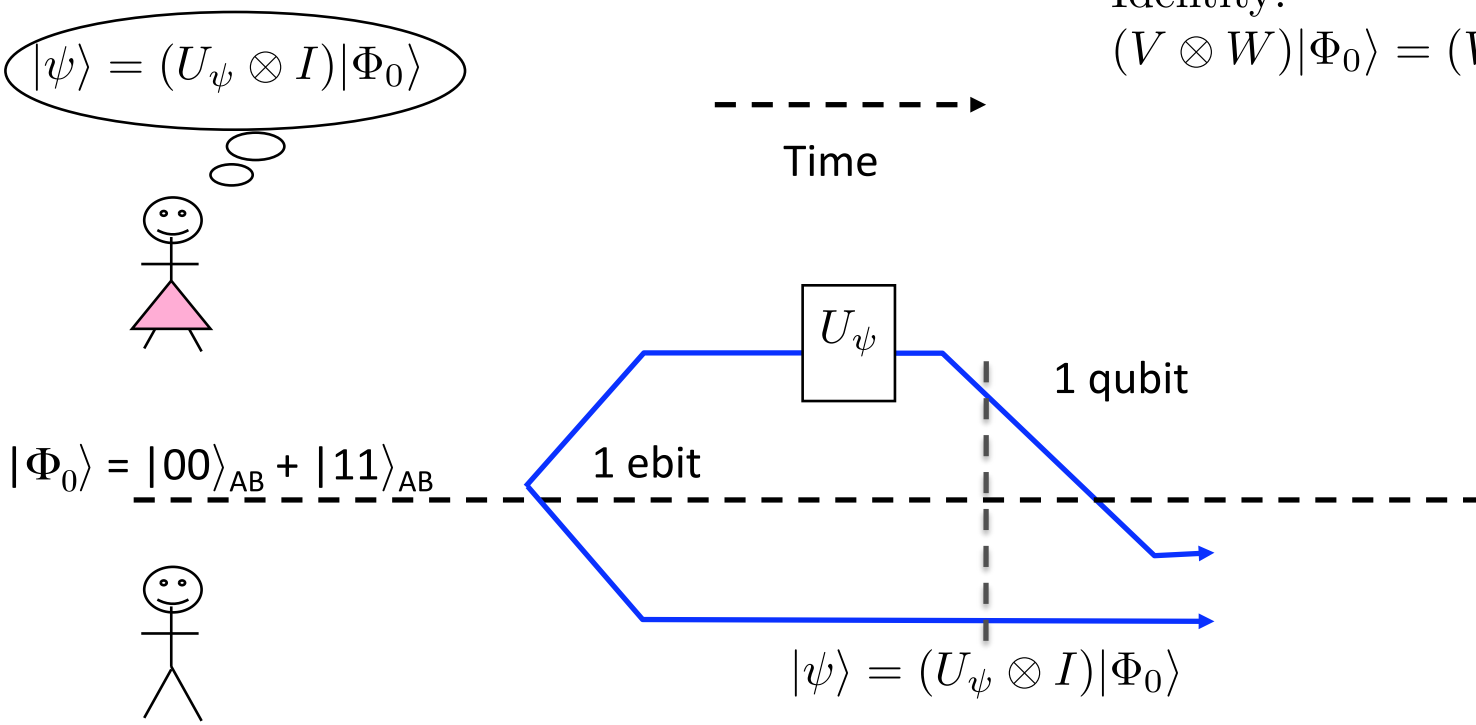
2 qubits + 2 ebits ≥ 4 qubits

Substitute: (1 qubit + 1 ebit) + 2 ebits ≥ 4 qubits
1 qubit + 3 ebits ≥ 4 qubits

Repeat: 1 qubit + (2^k-1) ebits ≥ 2^k qubits

Superdense coding of maximally entangled states

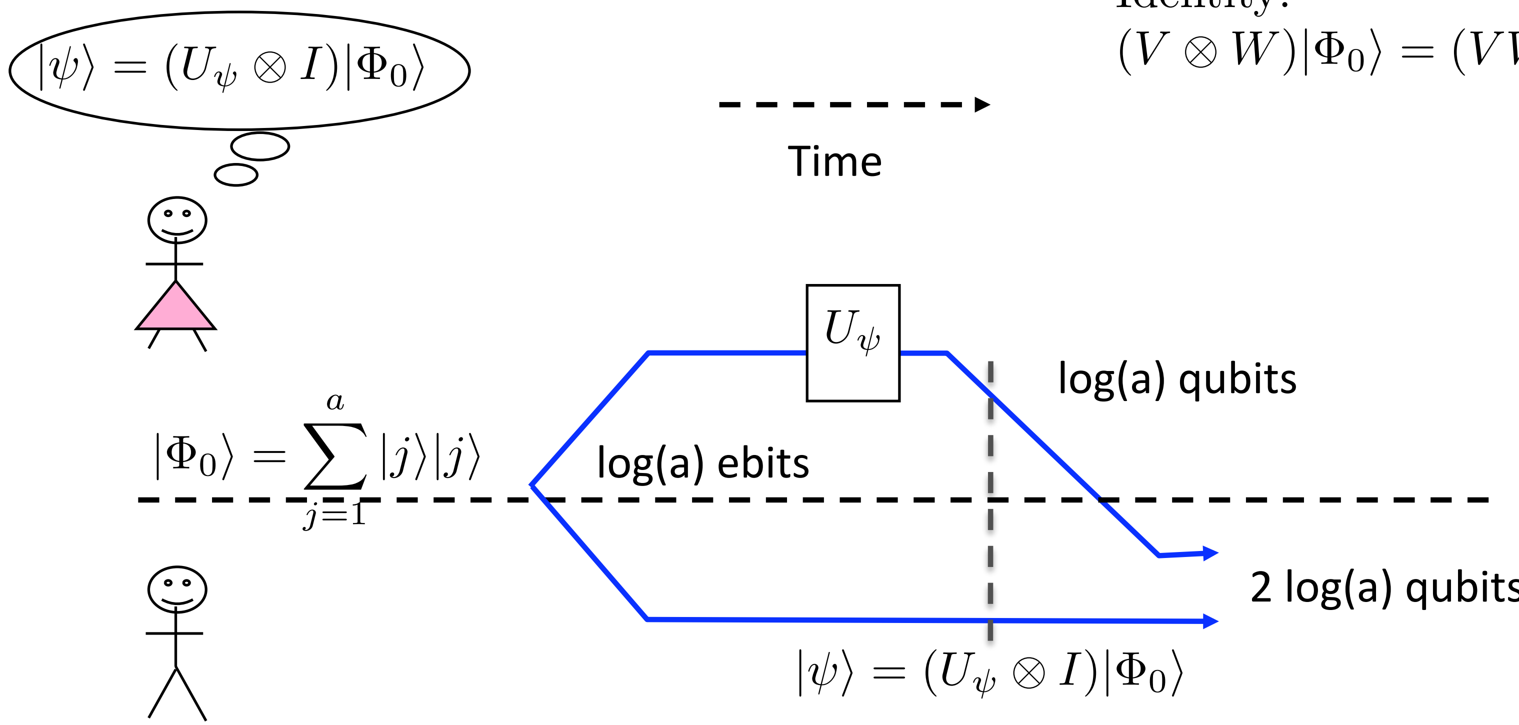
Identity:
$(V \otimes W)|\Phi_0\rangle = (VW^t \otimes I)|\Phi_0\rangle$



Alice can send Bob any maximally entangled pair of qubits by sharing an ebit and physically transmitting a qubit.

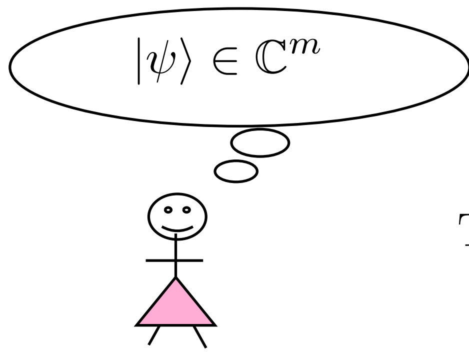
Superdense coding of maximally entangled states

Identity:
$(V \otimes W)|\Phi_0\rangle = (VW^t \otimes I)|\Phi_0\rangle$



Alice can send Bob and maximally entangled pair of qubits by sharing an ebit and physically transmitted a qubit.

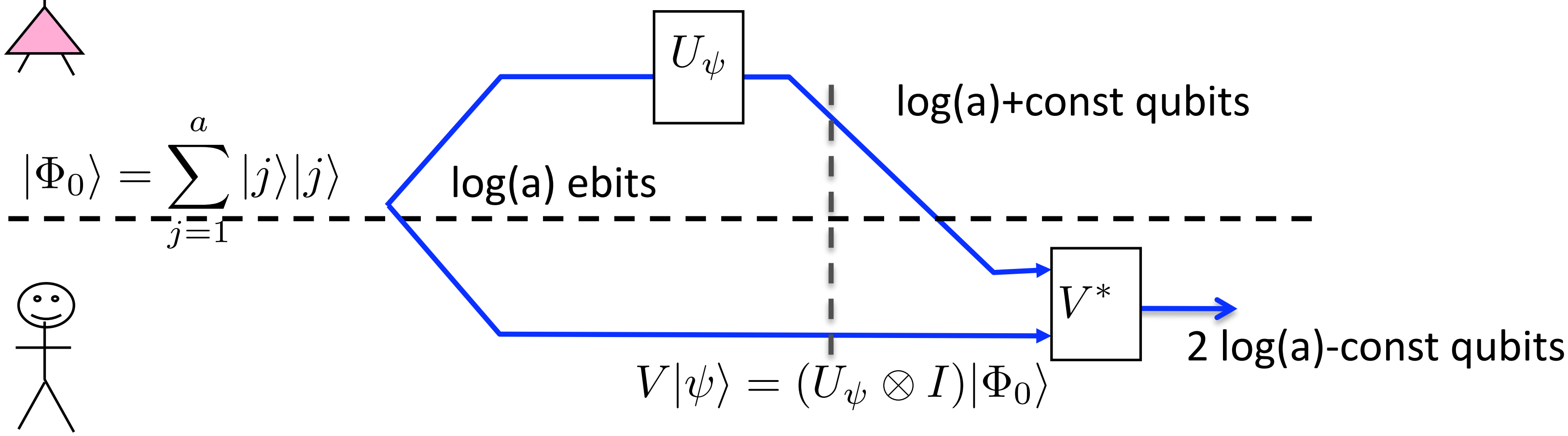
Superdense coding of arbitrary quantum states



Dvoretzky: $S \subset \mathbb{C}^a \otimes \mathbb{C}^b$ consisting only of almost maximally entangled states.

Let $V : \mathbb{C}^m \to S$ isometry.

There exists unitary U_ψ such that $V|\psi\rangle \approx (U_\psi \otimes I)|\Phi_0\rangle$.



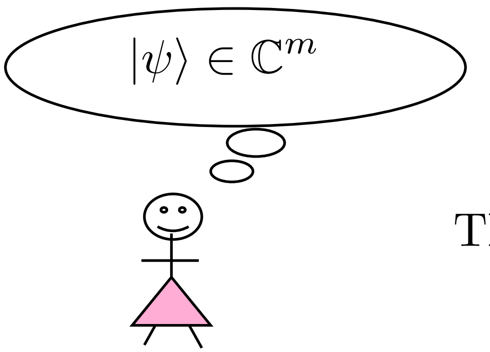
Asymptotically, Alice can send Bob an arbitrary 2 qubit state by sharing an ebit and physically transmitting 1 qubit.

1 qubit + 1 ebit ≥ 2 qubits

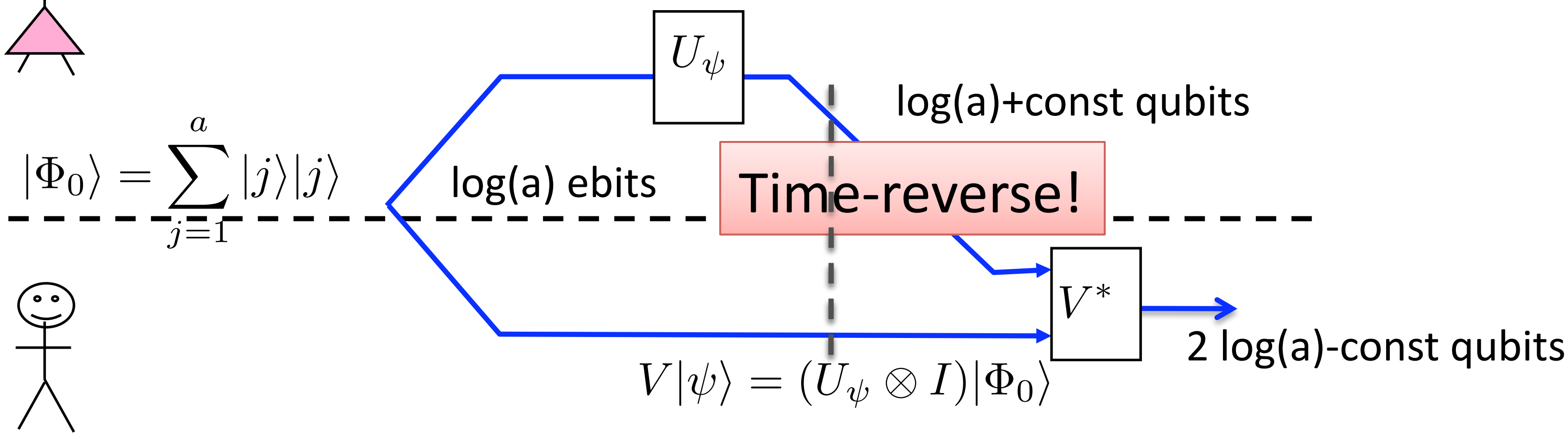
Approximate quantum one-time pad from superdense coding

Dvoretzky: $S \subset \mathbb{C}^a \otimes \mathbb{C}^b$ consisting only of almost maximally entangled states.

Let $V : \mathbb{C}^m \rightarrow S$ isometry.



There exists unitary U_ψ such that $V|\psi\rangle \approx (U_\psi \otimes I)|\Phi_0\rangle$.

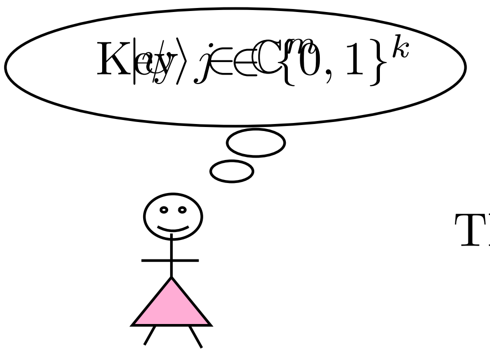


Asymptotically, Alice and send Bob an arbitrary 2 qubit state by sharing an ebit and physically transmitting 1 qubit.

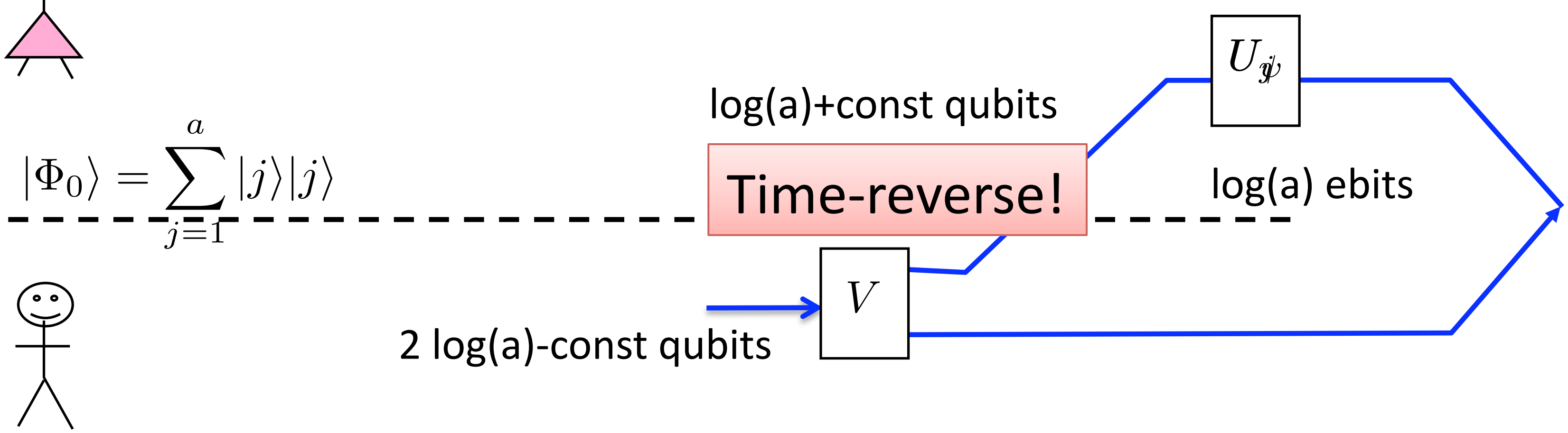
Approximate quantum one-time pad from superdense coding

Dvoretzky: $S \subset \mathbb{C}^a \otimes \mathbb{C}^b$ consisting only of almost maximally entangled states.

Let $V : \mathbb{C}^m \to S$ isometry.



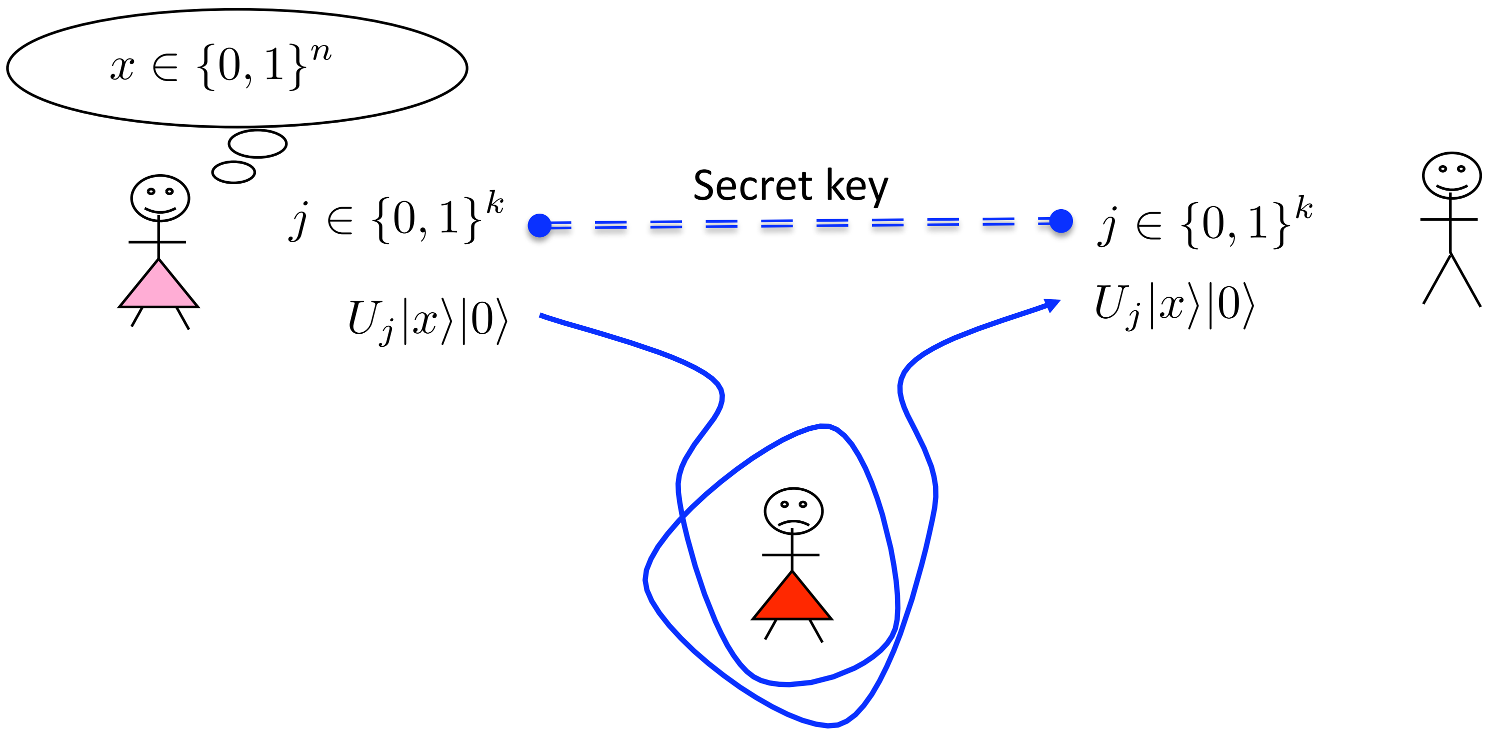
There exists unitary U_ψ such that $V|\psi\rangle \approx (U_\psi \otimes I)|\Phi_0\rangle$.



Asymptotically, Alice and send Bob an arbitrary 2 qubit state by sharing an ebit and physically transmitting 1 qubit.

$\{U_j\}$ forms a perfect quantum one-time pad: Total key required is 2 x (log(a) + const).

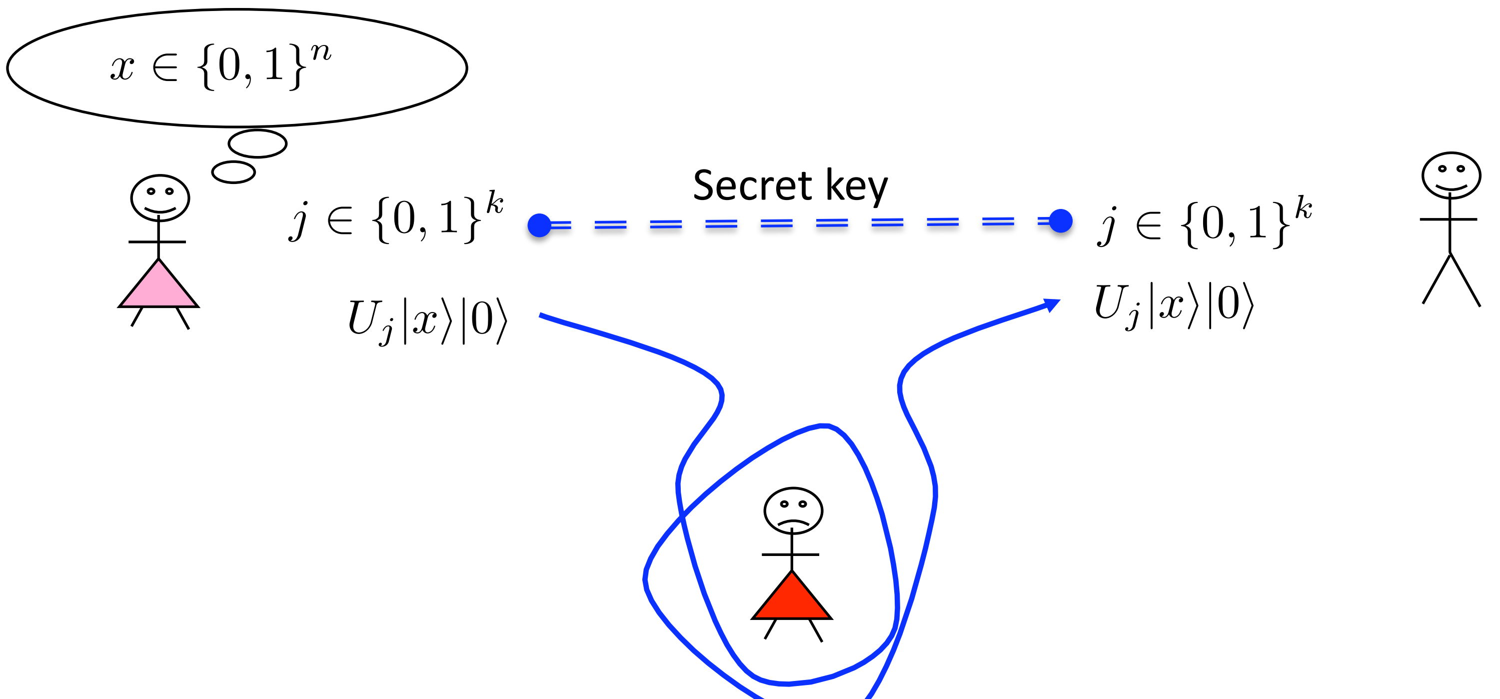
Encrypting classical bits in quantum states



Strongest security: for any pair of messages x_1 and x_2, Eve cannot distinguish the encrypted x_1 from the encrypted x_2. (TV ≤ δ)

Less strong security: Assume x uniformly distributed. Eve uses Bayes' rule to calculate p(x|measurement outcome).
TV from uniform ≤ δ for all measurements and outcomes.

Encrypting classical bits in quantum states



Less strong security: Assume x uniformly distributed. Eve uses Bayes' rule to calculate p(x|measurement outcome).
TV from uniform ≤ δ for all measurements and outcomes.

Colossal key reduction: Can take k = O(log 1/δ).
Proof: Choose $\{U_j\}$ i.i.d. using Haar measure, no ancilla.
Adversarial argument for all measurements complicated.

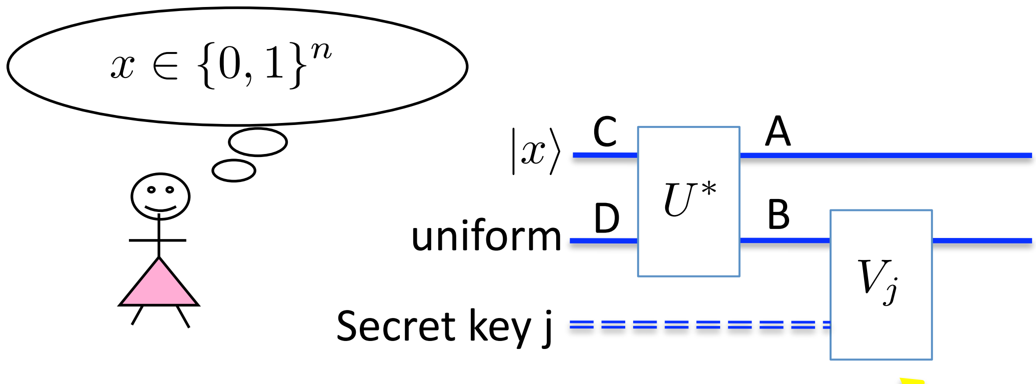
[HLSW03], [Dupuis-H-Leung10], [Fawzi-H-Sen10]

Quantum encryption of cbits: Connection to $\ell_1(\ell_2)$

Imagine $U : A \otimes B \to C \otimes D$ is unitary such that each $V_k : A \to C \otimes D$ given by $V_k|\phi\rangle = U|\phi\rangle|k\rangle$ and $|\phi\rangle \in A$ satisfy

$$\| V_k |\phi\rangle \|_{1,2} \geq (1-\epsilon)\sqrt{\dim C}\, \| V_k|\phi\rangle \|_2 \, .$$

Each V_k gives a low-distortion embedding of ℓ_2 into $\ell_1(\ell_2)$.



Quantum one-time pad

Proof that this works is an easy calculation. (Really!)

Leads to key size O(log 1/ε) with ancilla of size O(log n + log 1/ε)

[Fawzi-H-Sen 10]

Explicit constructions!

- Adapt [Indyk07] construction of ℓ_2 into $\ell_1(\ell_2)$ to produce a *quantum algorithm* for the encoding and decoding.
- Recursively applies mutually unbiased bases and extractors.
- Build Indyk embedding from an explicit sequence of 2-qubit unitaries.
- Procedure uses number of gates polynomial in number of bits n. (Indyk algorithm runs in time exp(O(n)).)
- Get key size $O(\log^2(n)+\log(n)\log(1/\varepsilon))$.
- Also gives efficient constructions of:
  - Bases violating strong entropic uncertainty relations
  - Efficient protocols for string commitment
  - Efficient encoding for quantum identification over cbit channels

Summary

- Basic problems in quantum information theory can be interpreted as norm embedding problems:
  - Approximate quantum one-time pad
  - Existence of highly entangled subspaces
  - Quantum encryption of classical data
  - **Additivity conjecture!** (Not even mentioned)
- Formulating problems this way simplifies proofs *and* allows application of known explicit constructions

Open problems

- Explicit constructions for embedding ℓ_2 into Schatten ℓ_p?
- Why do all these results boil down to variations on Dvoretzky?
  - What other great theorems should quantum information theorists know?